ChinaXiv合作期刊

基于国密区块链的融合媒体版权保护系统设计与实现

王怀营　曹三省
（中国传媒大学媒体融合与传播国家重点实验室，北京 100024）

摘　要：随着融合媒体时代的到来，数字媒体内容的传播越来越广泛，数字媒体产品的盗版和侵权行为极大地损害了媒体创作者的创作积极性和经济利益，中心化的版权保护方式已经难以满足数字时代版权保护的需要。区块链技术作为一种分布式记账技术的新兴技术，可以更高效地实现融合媒体版权保护要求。本文基于 Fabric 联盟链设计并实现了融合媒体领域的数字版权保护系统，将国密算法改造的 Fabric 应用到融合媒体数字版权保护系统中，满足当前对基于区块链的融合媒体数字版权保护技术的要求。

关键词：融合媒体；版权保护；区块链；国密算法 Fabric　　**中图分类号：**TP391　　**文献标识码：**A
文章编号：1671-0134（2022）04-128-05　　DOI：10.19483/j.cnki.11-4653/n.2022.04.039
本文著录格式：王怀营，曹三省 . 基于国密区块链的融合媒体版权保护系统设计与实现 [J]. 中国传媒科技，2022（04）：128-132.

chinaXiv:202310.00427v1

1. 背景和现状

1.1　数字版权保护技术研究现状

数字版权保护涉及的关键技术有加密技术、数字签名技术、可信计算技术等。例如在版权追踪溯源方面，主要是采用数字指纹技术 [1] 和数字水印技术 [2] 判断内容是否为盗版，为内容提供商的盗版追溯提供技术支撑。国内外很多企业以及科研院所都已获得了一批数字版权保护技术的核心专利，如国外的微软、索尼、三星等，国内的华为、中兴等公司以及清华大学和中国科学院等。

随着媒体融合的进一步发展，盗版问题屡见不鲜，传统版权保护方式已经很难解决当前的数字媒体内容保护问题，因此国内的许多研究人员也提出了关于数字媒体版权保护方面的研究。例如刘欣亮等人提出的面向开放互联网的多媒体数字版权保护系统 [3]、张婷提出的面向移动智能终端的多媒体版权保护系统的研究与设计 [4]、余芳提出的移动端的多媒体版权保护系统研究与实现 [5] 等。上述的方案大多还是基于第三方机构对于数字版权内容进行授权和验证，存在数据中心化管控的问题。并且融合媒体数字版权保护不能只关注加密和授权技术，而应该对媒体产品的整个发行过程进行保护，确保数字媒体内容在整个生命周期内得到合法使用。[6]

总体来说，数字版权保护技术还处于快速发展与不断创新阶段。随着数字网络技术的快速发展和应用、新兴业态的不断涌现，以及社会版权环境的不断改善，数字版权保护技术将得到更多重视和更大发展。

1.2　区块链技术研究现状

区块链技术带来的去中心化技术热潮引发了学术、产业界的高度关注 [7]，ITU、IETF、ISO 等国际组织确立区块链研究方向以探索技术标准化方向以及与应用的融合点，国内权威机构发布区块链标准规范、发展状况白皮书以指导区块链技术发展和应用。区块链的概念在 2008 年就已经由中本聪首次提出，但在近几年迎来了研究爆发期。2021 年我国的区块链行业专利申请数量达 15985 项，占全球申请总量的 84%，位居第一。[8] 目前区块链技术正在进入 3.0 时代。区块链的典型应用场景有金融服务、征信管理、版权保护、物流与供应链以及物联网等领域。[9] 在金融服务领域，国内的中国人民银行早在 2016 年就对外发布了积极关注区块链技术发展的消息，国外的许多国家，如美国、日本、加拿大、瑞典等均已经推出了以政府为主导的数字货币。在版权保护领域，中国搜索历时 4 年自主研发区块链技术，于 2021 年 1 月发布了“媒体融合链”区块链版权平台。[10]

2. 区块链相关理论

2.1　区块链技术

区块链是一种使用链结构和密码算法进行分布式数据存储的账本技术。可以将区块链看成是一种特殊的分布式数据库，用于维护公共数据账本。区块链由一系列区块组成，每个区块包含一个区块头和一个区块体。区块头用于链接前后区块并且保证历史数据的完整性，它记录了前一区块的 Hash 值、时间戳、随机数、Merkle 根等。根据比特币挖矿算法，节点（矿工）检验交易的有效性，竞猜随机数来解决数学难题，成功挖矿的节点将交易打包加入区块，并连接到区块链上最新的区块。前一区块的 Hash 值使得当前区块始终唯一地指向前一区块，从而形成区块链独特的链式结构。区块头中的随机数是矿工解决上述数学难题的解。其中 Merkle 根由所有交易数据的 Hash 值两两进行 Hash 计算后得出，能够总结并快速归纳校验区块中的某个交易被篡改，并且需要相应地改变区块头中的 Merkle 根以保证区块数据的完整性，再通过对区块头进行计算得到每个区块的唯一 Hash 值来代表此区块的独一无二性。区块体包含当前区块的交易数量和每个交易特定的哈希值，它们通过 Merkle 树的数据结

chinaXiv:202310.00427v1

构连接。区块链结构如图 1 所示。

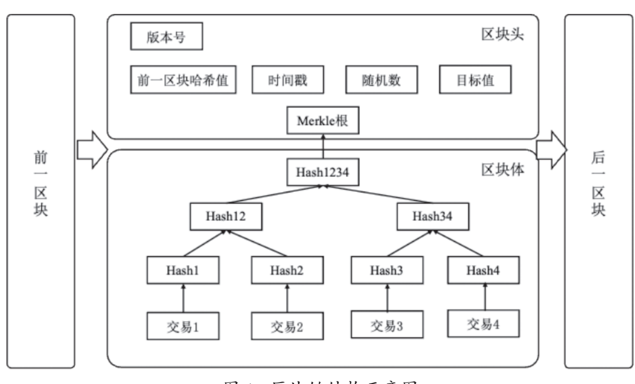


图 1　区块链结构示意图

2.2 联盟链及 Fabric 简介

联盟链是用于机构间的许可准入式区块链，只针对某个特定群体的成员和有限的第三方，虽然非完全的“去中心化”，但在效率和成本优化上具有优势 [11]，适用于构建媒体融合场景下的区块链版权保护系统。

Fabric 是一种联盟链的分布式操作系统，只有获得许可的用户才能在授权的通道上查询或调用交易，它为实现多用途分布式解决方案提供了一个安全、私有、灵活、可扩展的平台。由于无许可区块链对所有人完全开放，因此不利于保证所有参与者的隐私。与所有成员都可以参与的无许可区块链机制不同，提供特定访问机制的许可区块链可以确保数据只在系统指定的参与者之间流动。[12]Hyperledger Fabric 是目前最流行的许可区块链平台，它通过将系统划分为不同的通道，保证只有同一通道的参与者可以查看通道的数据，而不在通道的参与者不能进入通道。Fabric 使用即插即用的成员管理服务和共识服务运行，这些服务实现了可定制的智能合约的理念，以规范各方之间的交互。Hyperledger Fabric 架构图如图 2 所示。

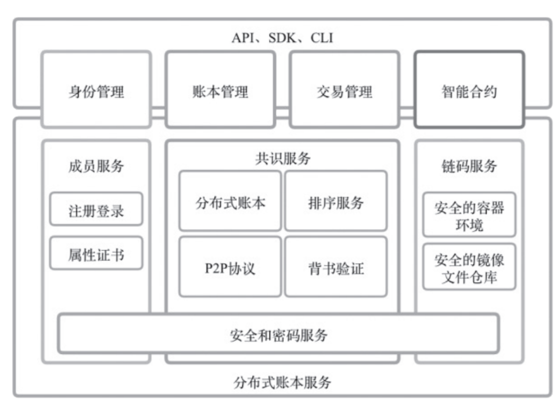


图 2　Hyperledger Fabric 架构图

3. Fabric 的国密化改造

3.1　可行性分析

密码算法是保障信息安全的核心技术，区块链技术的安全依赖于密码安全。区块链长期使用国际通用的密码算法体系和相关标准，如 SHA、RSA 等。为从根本上摆脱对国外密码技术和产品的过度依赖，国家密码管理局制定了一系列密码标准，包括 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 等。

在 Hyperledger Fabric 的交易过程中，每个阶段都应用了密码学算法。非对称加密算法主要用于在交易过程中验证节点的身份。为保证数据不被篡改，在数据签名和发证过程中采用单向哈希算法对数据进行哈希处理。对称加密算法在区块链的通信和隐私数据保护中发挥着重要作用。

2019 年 4 月，国家广播电视总局官网发布《县级融媒体中心网络安全规范》，该规范中的多项要求中指出在采用密码相关技术时要支持国密算法，基于国密算法对内容数据进行数字签名、验签，使其具备内容防篡改功能。从技术角度上来讲，Hyperledger Fabric 采用模块化设计方案，有助于实现密码模块的国密算法转换。

为了使版权保护技术适用于当前融合媒体的发展 [13]，满足国家在数字版权保护等广播影视重要领域开展国产密码应用的要求，本文将基于国产密码学标准，实现国密加解密、签名验签、哈希算法，并将其集成到 Fabric 平台，实现国密版 Fabric。Hyperledger Fabric 国密版支持主要体现在签名算法采用 SM2 椭圆曲线公钥密码算法，杂凑算法采用 SM3 密码杂凑算法，对称加密算法采用 SM4 加解密算法。

3.2　国密化改造方案

3.2.1　Hyperledger Fabric 底层密码学套件

为实现 Hyperledger Fabric 的国密化改造，需要先对其底层密码学套件进行分析，了解密码服务在 Fabric 中的加密机制。BCCSP（Blockchain Cryptographic Service Provider，即区块链密码服务提供者）是 Hyperledger Fabric 的加密服务提供者，它能够用来提供加解密、签名校验相关功能，并定义了系统所需的各种密码算法。系统上层应用模块中（如 MSP、cryptogen、CA、Fabric-SDK-Go 等）使用的密码算法都只是对 BCCSP 中定义的密码算法的调用。另外，不同的模块也会根据需要来定义特定使用的密码模块。

从图 3 中可以看出，BCCSP 通过 MSP（Membership Provider Service）向核心模块以及客户端 SDK 提供加密算法相关服务。MSP 是基于数字证书的成员身份管理，通过调用 BCCSP，即证书服务，来完成签名验签等功能。Fabric 提供国密算法服务的同时需要使用基于国密的数

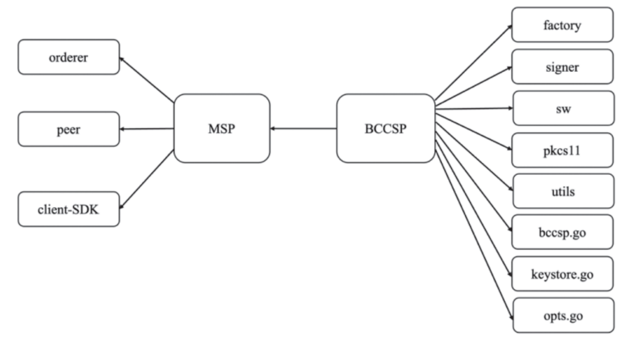


图 3　BCCSP 结构

ChinaXiv合作期刊

chinaXiv:202310.00427v1

字证书服务，以便使用数字证书时能够验证国密的数字签名，从而辨别用户身份。BCCSP 模块对上层抽象出了区块链密码服务，包含非对称加密、对称加密、数字签名算法、哈希计算，以及各种算法对于密钥的生成和导入。不同的加密算法需要实现 BCCSP 中定义的接口，以向上层提供加密服务。在 BCCSP 中实现了一种对称算法（AES）和两种公钥算法（RSA 和 ECDSA）。使用 AES 加密明文时，pkcs7 用于填充明文，然后使用 CBC 模式加密明文。解密时用 CBC 解密，pkcs7 用于恢复明文。RSA 和 ECDSA 的密钥结构和签名加密算法分别由 crypto/rsa 和 crypto/ecdsa 实现。通过 BCCSP 可以实现 Fabric 中的可插拔密码算法模块，BCCSP 密码服务套件是改造 Hyperledger Fabric 底层密码套件的突破点。

3.2.2 架构设计

由上一节中对 Fabric 底层密码学套件的分析，可以得出 Fabric 国密化改造会涉及到的模块如图 4 所示。

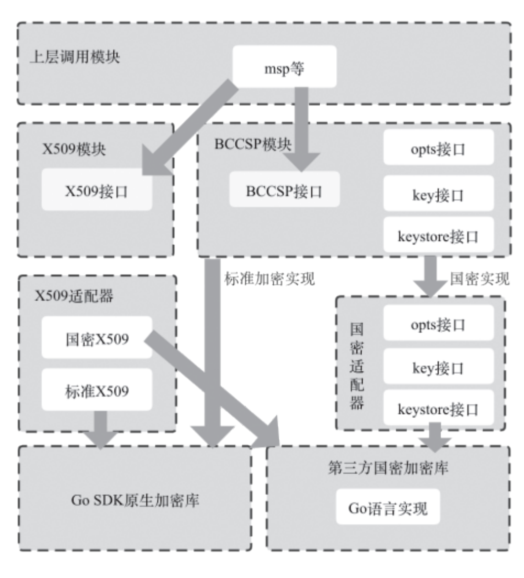


图 4 Fabric 国密改造涉及的主要模块

其中上层调用模块主要是由 MSP 等模块为 Fabric 提供成员加密服务，它的实现依赖于 BCCSP 模块和 X509 模块。

BCCSP 模块主要实现了四套接口，分别是 BCCSP 接口、opts 接口、key 接口以及 keystore 接口。其中以 BCCSP 接口为主，它包含了加解密、签名验签等主要方法。其他三套接口为辅，它们主要包含用于密钥管理和存储的一些方法。BCCSP 模块有两套实现方式，一套是标准加密，它直接依赖于 GoSDK 原生的加密库，另一套是国密实现，需要依赖于第三方的提供的底层加密库，一般分为硬实现和软实现两种方式，其中硬实现就是加密机，软实现采用 Go 语言实现。由于实验条件的限制，本文选择软实现的方式实现国密加密库。由于 Fabric 定义的 BCCSP 接口并不直接兼容于第三方提供的加密接口，因此需要做一个国密适配器，主要用于适配上层的 BCCSP 模块和底层的第三方加密库，这个国密适配器主要包含了 SM2、SM3 以及 SM4 三种国密算法的适配。

X509 模块主要提供的是有关证书的一系列方法。Fabric 默认是使用标准 X509 的，底层直接调用的是 Go SDK 原生的加密库。为了让 X509 支持国密的同时也兼容标准加密，可以把证书相关的接口抽象出来定义为 X509 接口，然后底层采用标准加密和国密。标准加密依旧是直接调用原生 Go SDK 标准加密库，而国密则是调用第三方的国密库，以此来实现国密算法的可插拔式。启动区块链网络时可根据实际需求通过在 Orderer、Peer 和 CLI 的配置文件中的配置项来指定使用国密或标准加密算法。

3.3 国密化改造实现

3.3.1 Hyperledger Fabric 底层密码学套件

本次 Fabric 国密化改造中所涉及到的加密算法主要是 ECDSA 签名算法、SHA256 杂凑算法以及 AES 对称加密算法，它们是由 Golang 底层的标准库 crypto 包实现的。参考 Fabric 原有的加密算法的实现，将国密算法在 Fabric 中的具体实现分为以下 6 个步骤：

1）在 crypto 模块中定义 SM2 公私钥的基础类型，即 SM2 公钥和私钥的构造函数。将公钥定义为 PublicKey，将私钥定义为 PrivateKey。

2）实现国密适配器 gmsm 分为三个接口的实现，分别是：SM2 接口、SM3 接口、SM4 接口。其中 SM2 接口主要包含密钥生成、签名、签名验证、加密、解密等方法，SM3 接口主要包含计算数据摘要等方法，SM4 接口主要包含用 SM4 对称密钥加解密等方法。

3）在 BCCSP 模块实现国密工厂类型 GMFactory，使用创建出的国密工厂类型调用 initBCCSP 方法初始化 BCCSP 对象。

4）在 x509 模块中定义证书类型结构体。本模块涉及两套实现，分别是国密证书库 gmX509 和标准证书库 standX509。gmX509 通过对第三方 x509 库进行封装实现，standX509 通过对 GoSDK 原生的 x509 库进行封装实现。

5）完成 Fabric 源码中密码函数包的 SM2、SM3、SM4 算法替换后，将这些重新设计的密码函数包封装在国密插件中，再将国密插件嵌入到 BCCSP 的底层实现中。然后改变各个模块中密码算法相关部分的调用方式，使这些调用指向 BCCSP 模块中的国密插件提供的国密接口，从而实现各个上层应用对国密算法的调用支持。

6）如果使用国密算法，需要针对参数（比如 gmsm）加载对应的国密插件，调用 InitGMPlugin 方法，初始化 SM2、SM3 和 SM4 三个结构体，否则不会加载国密插件，默认指定为非国密。

3.3.1 扩展 BCCSP 模块

前文已经对相应的国密算法进行了实现，本小节将对 BCCSP 模块进行国密扩展，添加国密插件。

BCCSP 在 Fabric 中用来提供相关的密码标准及其实现。BCCSP 模块包含一些重要的接口，其中涉及到密钥操作、哈希散列、签名验签、加密解密等一些关键操作。

chinaXiv:202310.00427v1

在该模块中，BCCSP.go 所定义的 BCCSP 接口需要借助前面实现的国密适配器中提供的国密算法相关接口来实现相应的接口功能。

BCCSP 接口中主要包含以下方法，如表 1 所示。

表 1　基于国密改造的 BCCSP 接口方法实现

接口类型	方法定义	方法说明
密钥生命周期的管理	KeyGen（opts KeyGenOpts）（k Key，err error）	根据输入参数 KeyGenOpts 来选择具体生成哪种类型的密钥
	KeyDeriv（k Key，opts KeyDerivOpts）（dk Key，err error）	根据密钥 k，派生出新的密钥，国密暂不需要支持此接口，直接返回空即可
	KeyImport（raw interface{}，opts KeyImportOpts）（k Key，err error）	用于导入密钥，由 opts 指定密钥类型
	GetKey（ski []byte）（k Key，err error）	从文件路径读取密钥实例
哈希散列的函数管理	Hash（msg []byte，opts HashOpts）（hash []byte，err error）	实例化 SM3 对象，并利用该对象对原始数据进行哈希
签名验签的算法管理	GetHash（opts HashOpts）（h hash.Hash，err error）	只会实例化 SM3 对象，然后由外部选择调用 SM3 的哈希方法
	Verify（k Key，signature，digest []byte，opts SignerOpts）（valid bool，err error）	调用 SM2 实例的 Verify 接口来对数据及摘要进行验签
加密解密的算法管理	Encrypt（k Key，plaintext []byte，opts EncrypterOpts）（ciphertext []byte，err error）	调用 SM2/SM4 实例的 Encrypt 接口来对数据进行非对称 / 对称加密
	Decrypt（k Key，ciphertext []byte，opts DecrypterOpts）（plaintext []byte，err error）	调用 SM2/SM4 实例的 Decrypt 接口来对数据进行非对称 / 对称解密

4. 融合媒体版权保护系统总体设计与实现

4.1　系统设计概述

本系统主要为媒体行业的融合媒体数字版权保护场景提供解决方案，数字版权作品类型包括文本、视频、音频、图片，应用场景，如图 5 所示。本系统的服务对象主要有原创机构、企业自媒体、原创媒体以及个人创作者。原创机构是指报社、杂志社、原创图片网站等；原创媒体是指文章作者、原创自媒体、摄影师、插画师等原创个体；企业自媒体是指微信、微博、头条号等原创运营者以及企业账号等运营者。

系统设计实现的主要目的是，充分利用区块链的优良特性，为融合媒体数字版权创建一个安全可信的计算执行环境。[14] 同时基于国密版 Fabric 联盟链作为本系统的区块链服务层，构建一个集版权存证、交易、查询溯源为一体的系统，为融合媒体数字版权交易提供一个弱中心、去第三方、透明公开的安全可信平台。本系统基于经过国密改造的 Fabric 实现，使得版权保护系统满足国家在数字版权保护领域开展国产密码应用的要求。

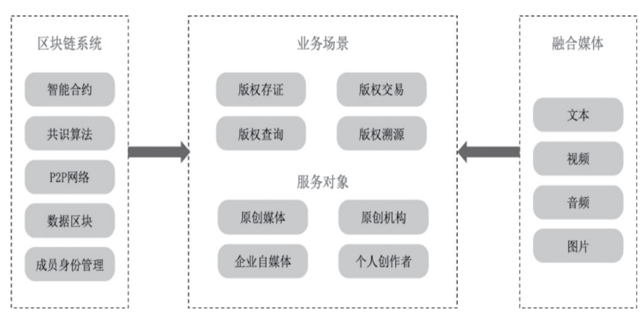


图 5　基于区块链的融合媒体数字版权保护系统应用场景

4.2　区块链网络设计

本系统利用 Hyperledger Fabric 开源框架来搭建联盟链网络。该网络包含两个组织，每个组织都包含相关组件。网络节点架构示意图如图 6 所示。

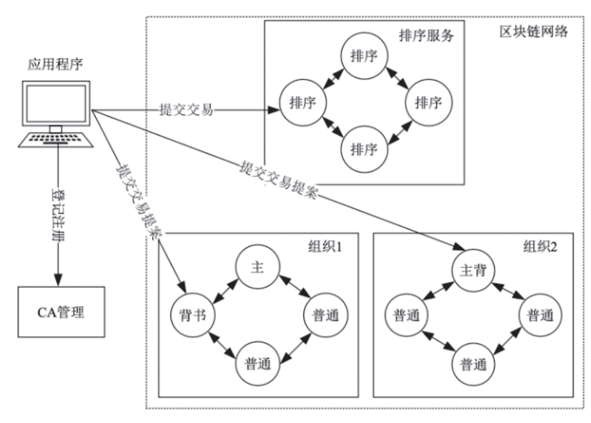


图 6　网络节点架构示意图

在本系统的链码设计中，抽象出以下功能函数，实现区块链环境下融合媒体数字作品的版权保护功能，以满足版权存证和溯源的需求。本文在链码中设计的主要功能函数如表 2 所示。

以上函数中，最核心也是最复杂的应该是媒体作品的版权交易，版权交易函数伪代码如下：

workExchange（ownerId，DigitalrightId，currentOwnerId）{

newOwner=currentOwnerId；　// 获取版权转让人

oldOwner=owneId；　// 获取版权被转让人

deleteoldOwnwe.list（）；　// 更新转让方版权列表

changeOwnerOfWork.Owner（）=newOwner；　// 媒体作品版权转让

chinaXiv:202310.00427v1

表 2　链码主要功能函数设计

函数名	输入参数	功能
userVerify ( )	(name，IDnumber)	用于实现系统新用户的认证，IDnumber 为身份证号
DigitalrightEnroll ( )	(DigitalrightName，DigitalrightId，Metadata，ownerId)	媒体作品交易对象的用户 ID
DigitalrightExchange ( )	(ownerId，DigitalrightId，currentOwnerId)	媒体作品交易时间
queryUser ( )	(ownerId)	用于查询用户及其版权作品的信息
queryDigitalright ( )	(DigitalrightId)	用于查询版权作品的详细信息
queryDigitalrightHistory ( )	(DigitalrightId)	用于查询版权作品的所有交易记录

```
updatenewOwner.list ( ) ;  // 更新被转让人版权列表
updateDigitalrightHistory ( ) ;  // 更新版权转让历史记录
}
```

通过系统各节点相应链码的 shim API 中的函数方法来获取或写入账本数据。本系统的链码由 Go 语言编写。在链码实现之前需要将账本数据映射为编程语言数据结构，以实现对数据对象的处理。以媒体版权作品对象为例，定义媒体版权作品对象为：

```
type Digitalright struct {
Name string `json: " name" ` // 媒体版权作品名称
Id  string `json: " id" ` // 媒体版权作品编号
Type string `json: " type" ` // 媒体版权作品类型
Time string ‘json: " time" ’ // 媒体版权生成时间
Metadata string `json: " metadata" ` // 媒体版权 hash 值
}
```

4.3　系统实现

本系统选择 Hyperledger Fabric 联盟链作为实施平台，初步实现了“版权登记”“版权信息查询”“版权转让”“版权交易记录查询”等功能，基本满足了融合媒体版权保护系统功能需求。其中系统版权登记界面效果如图 7 所示：

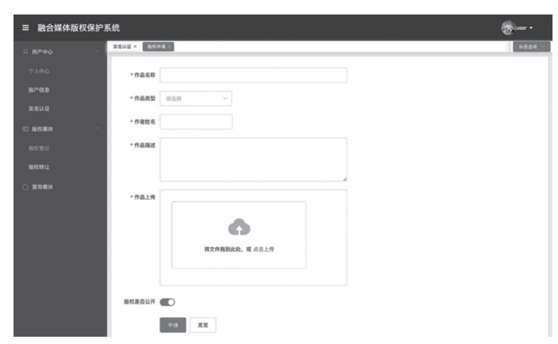


图 7　版权登记界面

结语

区块链因其不可篡改、可追溯、去中心组织化的特性，可以被应用到版权保护领域之中，为媒体资源的版权保护提供基础技术支持，从而解决传统版权保护方式存在的安全性差、交易流程复杂、成本高等问题。通过实现对 Fabric 支持国密算法的改造，满足当前对基于区块链的融合媒体数字版权保护技术的要求。另外，侵权行为的实时检测也是版权保护研究的一个重要环节，这一环节目前无法只使用区块链技术自身来实现，可以通过引入大数据分析、人工智能、网络爬虫等其他计算机技术，实现对大部分盗版行为频繁发生的网站甚至整个互联网范围的实时版权监测，从而更好地保护版权。媒

参考文献

[1] Gold，Steve. Understanding the digital fingerprint [J]. Network Security，2013 (12) ： 15−8.

[2] Zhuang J Z. Digital Watermarking Technology [J]. Computer Knowledge and Technology，2009.

[3] 刘欣亮，黄涛，张志勇 . 面向开放互联网的多媒体数字版权保护系统 [J]. 计算机工程与设计，2015 (2) ： 363−368.

[4] 张婷 . 面向移动智能终端的多媒体版权保护系统的研究与设计 [D]. 北京：北京邮电大学，2018.

[5] 余芳 . 移动端的多媒体版权保护系统研究与实现 [D]. 北京： 北京邮电大学，2016.

[6] 陈志业，罗泽文，张智骞，冉大为，姜堑，王兵 . 新媒体环境下数字版权保护集成技术研究 [J]. 广播电视信息，2020 (S1) ：63−67.

[7] 邵奇峰，金澈清，张召，钱卫宁，周傲英 . 区块链技术：架构及进展 [J]. 计算机学报，2018 (5) ：969−988.

[8] 陈丽姗 . 中国区块链专利数据报告(2021)[EB/OL].(2022) [2022]. http：//www.01caijing.com/article/309236.htm

[9] 曾诗钦，霍如，黄韬，刘江 , 汪硕 , 冯伟 . 区块链技术研究综述：原理、进展与应用 [J]. 通信学报，2020 (1) ：134−151.

[10] 赵丹文 . 新华社利用区块链技术在版权保护方面的探索 [J]. 中国传媒科技，2021 (10) ：138−141.

[11] 陈晓峰，王子欣，解庆 . 区块链技术在广播电视内容审核场景下的应用研究 [J]. 中国传媒科技，2021 (11) ：7−9.

[12] 李晓芳 . 多通道联盟链关键技术研究与实现 [D]. 成都：电子科技大学，2020.

[13] 郭宇宁，曹建香，林卫国 . 从机制到架构理解 China 数字版权管理系统 [J]. 广播电视信息，2019 (S1) ： 6−8.

[14] 彭桂兵，吴基祥 . 区块链技术在媒体版权保护中的应用与反思 [J]. 出版发行研究，2020 (8) ： 73−80+18.

作者简介： 王怀菅(1997−)，女，山东聊城，硕士研究生，中国传媒大学媒体与融合传播国家重点实验室、信息与通信工程学院，研究方向：全媒体与网络视听监管技术；曹三省 (1977−)，男，山东临清，研究员，中国传媒大学媒体与融合传播国家重点实验室、协同创新中心，研究方向：媒体融合与智能媒体。

（责任编辑：陈旭管）